Aiello 1999-0053

REMARKS

A telephone interview was held with Examiner David Jung, who reportedly is now the Examiner of record. Mr. Jung noted that

- numerous Examiners had handled the case in the past,
- a review of the actions reveals that the previous Examiner was somehow confused,
- the previous Office Action (OA) is vacated – as if it had not been lodged in the first place,
- consequently applicants' response to the previous OA is as if not filed at all,
- the current OA is a new FINAL OA, and
- the statutory 6-month clock has been reset.

No substantive discussion was held, but it was agreed that because of the checkered past of this case's handling, the Examiner will seriously consider entering this claim even if substantive amendments are made to the claims.

The Examiner's forthright and open discussion of the handling history of this case, and his kind agreement to enter this amendment are greatly appreciated. It so happens that such handling also comports with the directive in the current Office action to correct a typographical error in the specification, but this does not take away from the Examiner's commendable approach.

The claims are amended herein to correct a few minor typographical errors that arose from the previous amendment to the claims, and to clarify that the defined steps are executed in order. Substantively, the claims are as presented following applicants' April 30, 2004 response to the first OA, *and as apparently treated by the Examiner*. No change has been made in an effort to overcome the prior art.

Claim 1 was rejected in the first OA under 35 USC 102 as anticipated by Reed III et al, U.S. Patent 5,153,919. This rejection is repeated verbatim in the outstanding FINAL OA, with a comment in the "Response to Arguments" section of the OA that addresses applicants' previous arguments.

Regarding the first clause of the method defined in claim 1, the Examiner asserts that the Reed III et al references discloses "authenticating a provisioning server (base station, Reeds, col. 3, lines 21-23)." However, the cited text states:

PAGE 11/18 * RCVD AT 4/25/2005 2:10:49 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/9 * DNIS:8729306 * CSID:9734676589 * DURATION (mm-ss):07-54

> Thereafter the mobile unit communicates with the base station with the assistance of authentication processes that are carried out between the mobile unit and the base station, using the shared secret data field.

Respectfully, the fact that a shared secret data field (crypto-key) exists, or that a crypto-key is used to communicate securely between a mobile unit (A) and a base station (B) does not demonstrate that B is, or was, authenticated to A, or even that A was authenticated to B. There is certainly no *ipso facto* mutual authentication to each other. To illustrate, B – who could be anyone – could have simply given the crypto-key to A.

Accordingly, it is respectfully submitted the cited passage does not support the Examiner's first OA assertion that there is an authentication of the base station, and does not support the Examiner's "Response to Arguments" assertion that there is *mutual* authentication. The Examiner's assertion fails and, consequently, claim 1 is believed to be not anticipated by Reed III et al.

The above notwithstanding, applicants wish to address an argument that could have been made, which is that the creation of the RANDBS string by the mobile unit and the base station's AUTHBS response is an authentication of the home CGSA (FIG. 2 of the reference).

The process disclosed by Reed III et al in connection with FIG. 2 is:

(a) the mobile unit creates a RANDBS string, and sends it to the home CGSA,

(b) the home CGSA creates an AUTHBS string and sends it to the mobile unit,

(c) the mobile compares the AUTHBS string received from the home CGSA to an AUTHBS created within the mobile unit and sends the comparison results to the home CGSA, and

(d) the home CGSA acts on the received comparison results.

While, as suggested above, an argument may be made that the process of comparing the two AUTHBS strings effect a mutual authentication, applicants respectfully submit that, in this case, that is **not** an authentication of the home CGSA because no action is taken by the mobile unit based on the results of the comparison. An authentication process is a process when one action is taken when the process reaches one result, and another action is taken with the process reaches the opposite result. Since no action is taken by the mobile unit based on the result of the above-described process, it follows that the mobile unit is NOT authenticating the home CGSA (base station, provisioning server).

Applicants respectfully submit, therefore that Reed III et al do not teach a step of authenticating the base station (as asserted by the Examiner) and, therefore, claim 1 is not anticipated by Reed III et al.

Moreover, if it is assumed (albeit, wrongfully) that the RANDBS/AUTHBS challenge-response process is a step of authenticating the base station, then it must follow that the step of "receiving information authenticating a provisioning server," specified in claim 1, must correspond to the step of receiving the AUTHBS string. In such a case, pursuant to claim 1 there must be additional steps to the method; to wit, the steps of (a) establishing a communication channel over which authorization information is transmitted from the user to the server, and (b) encrypting and transmitting cryptographic key to the provisioning server. If the Examiner were to make the assertion that the act of comparing the AUTHBS strings corresponds to the first clause of claim 1, then the observation would have to be made that there are no such additional steps. Therefore, again, claim 1 is not anticipated by Reed III et al even when just the first clause of claim 1 is considered.

In connection with the second clause of the method defined by claim 1, the Examiner asserts that the Reed III et al reference discloses establishing a communication channel between the user and the provisioning server over which authorization information is transmitted from the user to the provisioning server, citing col. 8, lines 60-61. The cited passage states:

> The mobile unit alters the SSD field and sends a challenge to the serving base station.

Respectfully, that does not support the Examiner's assertion. First, the challenge string is part of the process that is assumed (albeit wrongfully) to be the authenticating step. It is not a separate step of sending any information to the base station. Second, the sent challenge does not constitute authorization information in any sense of the word, because it does not authorize anything. It does not prevent the base station from doing anything. Even an argument which says that failing to send the RANDBS string causes the base station to not send the AUTHBS string is irrelevant, because failure to send the AUTHBS string makes no difference to the mobile unit, and the failure by the base station to receive a proper confirmation signal as a result of its own failure can be simply ignored. To repeat, the sent challenge does not constitute an "authorization information" in any

PAGE 13/18 * RCVD AT 4/25/2005 2:10:49 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/9 * DNIS:8729306 * CSID:9734676589 * DURATION (mm-ss):07-54

sense of the word. Therefore, the Examiner's assertion relative to the second clause of claim 1 fails, and that represents another, independent, reason to conclude that claim 1 is not anticipated by Reed III et al.

As to the third clause of claim 1, the Examiner asserts based on col. 6, lines 14 that the step of encrypting and transmitting a cryptographic key (SSD) is taught by Reed III et al. The sentence that includes cited passage states:

> The SSD field comprises two subfields: the SSD-A subfield which is used to support authentication procedures, and the SSD-B subfield which is used to support voice privacy procedures and encryption of some signaling messages (described below).

That, of course, merely states what the SSD field is, and provides no teaching to support an assertion that any cryptographic key is encrypted and transmitted to the home CGSA, as specified by claim 1. In fact, neither the SSD field nor any subfield thereof is sent by or to the provisioning server. The keys are independently generated within both the home CGSA and the mobile unit, *and that is precisely opposite from what the Examiner asserts*. It is respectfully submitted, therefore, that the third step of claim 1 is not found in the reference and that this fact forms yet another independent reason to conclude that Reed III et al does not anticipate claim 1.

Claims 2-11 depend on independent claim 34, and so do claims 35-39. It is appropriate, therefore, to address claim 34 at this juncture.

Claim 34 was rejected under 35 USC 102 at being anticipated by Weinstein et al, US Paten 6,094,485. Applicants respectfully traverse.

Weinstein et al describe the "SSL step up" process, which is a process that interacts with an SSL client that is permitted to employ a stronger key by expanding the available set of encryption algorithms to include stronger algorithms/key lengths. Basically, the Examiner appears to use the Weinstein reference because it involves a certification of the server as a step is deciding whether use of the cryptographically stronger algorithm is permitted.

Claim 34 (even in its unamended form) specifies receiving a key of the provisioning server, and information that authenticates the provisioning server. The Examiner asserts that Weinstein et al teach this limitation at col. 13, lines 38-39, but applicants respectfully disagree. The cited passage states:

PAGE 14/18 * RCVD AT 4/25/2005 2:10:49 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/9 * DNIS:8729306 * CSID:9734676589 * DURATION (mm-ss):07-54

> Following the hello messages, the server sends its certificate 36, if it is to be authenticated.

The sending of certificate 36 can be viewed as the sending of information that authenticates the provisioning server, but it clearly is not a message that includes both a key of the server and information that authenticates the server. In fact, the very next sentence of the text suggests that in some circumstances, based on the certificate of the server or lack thereof, another message may be sent, which is a "server key exchange" message. This sentence in the reference supports applicants' argument that there is NO received message that includes both "a key of said provisioning server and information that authenticates said provisioning server." It is respectfully submitted, therefore, that since the step of "receiving a key of said provisioning server and information that authenticates said provisioning server" is not taught by Weinstein et al, claim 34 is not anticipated by Weinstein et al.

The following step in claim 34 (even in its unamended form) specifies that the BTI generates a

1. key K and its complement (K^{-1}),
2. a key SK and its complement (SK^{-1}), and
3. a key AK and its complement (AK^{-1}).

The Examiner asserts that Weinstein et al teach this limitation, and in support of the assertion the Examiner points to col. 8, lines 1-4 and col. 10, line 46 with respect to K and K^{-1}, *points to no text whatsoever* with respect to SK, SK^{-1}, AK, AK^{-1}, and points to col. 4, lines 65-67 for the notion of a complement of a key J^{-1} being able to decrypt what was encrypted with a key J.

The passage at col. 8, lines 1-4 merely teaches that one of the cryptographic operations within SSL is stream cipher encryption, and that in such encryption plaintext is Exclusive ORed with a string obtained from encrypted output of a pseudorandom number generator. Respectfully, the developed string – being as long as the plaintext and, hence, of un-predetermined length – is not considered to be a random key (K) by Weinstein et al, and applicants respectfully submit that no artisan would consider that to be an encryption key. If, nevertheless, the Examiner chooses to consider that string as a key that is generated, then the Examiner must show that the BTI also develops the complement of this string (string K^{-1}) to serve as a decryption key. No such showing was

PAGE 15/18 * RCVD AT 4/25/2005 2:10:49 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/9 * DNIS:8729306 * CSID:9734676589 * DURATION (mm-ss):07-54

made. Clearly, the passage at col. 10, line 46 – which merely says "the decryption functions reverse the process" – teaches no such key. Moreover, such a choice by the Examiner must be accompanied by a showing, pursuant to the following step in claim 34, that this string K^{-1} is encrypted with the server's key and sent to the server, together with other information. That is not taught by the reference, and not even asserted by th Examiner. Consequently, it is respectfully submitted that the second clause of claim 34 is not taught by Weinstein et al, and this fact forms another reason to conclude that claim 34 is not anticipated by Weinstein et al.

As for generating SK, SK^{-1}, AK, AK^{-1}, even the Examiner has found no passages in Weinstein et al that teach the creation of these keys and their complements. This fact forms yet another reason to conclude that claim 34 is not anticipated by Weinstein et al.

The following step of claim 34 specifies sending to the provisioning server information that includes:

(a) K^{-1} encrypted with said key of said provisioning server, and

(b) a tuple encrypted with said K, which tuple includes SK^{-1} and AK^{-1}.

In support of the assertion that this step is also taught by Weinstein et al the Examiner points to col. 19, lines 16-22. The cited passage states:

> RSA Encrypted Premaster Secret Message.
>
> If RSA is being used for key agreement and authentication, the client generates a 48-byte pre-master secret, encrypts it under the public key from the server's certificate or temporary RSA key from a server key exchange message, and sends the result in an encrypted premaster secret message.

In terms that most closely resemble the claim 34 step, the above means that the client generates a 48-byte K^{-1}, encrypts it with a key from the server, and sends the results. This "most closely resembling" interpretation fails in it correspondence, however, because the 48-byte pre-master secret does not correspond to K^{-1}, because K^{-1} is created as a pair K, K^{-1}, and the reference does not show such a pair. Moreover, the cited passage completely ignores the claim portion relative to "the tuple encrypted with said K," which tuple includes SK^{-1} and AK^{-1}. It is respectfully submitted, therefore, that the claim 34 step of sending is not taught be Weinstein et al, and that this fact forms still another reason to conclude that claim 34 is not anticipated by Weinstein et al.

PAGE 16/18 * RCVD AT 4/25/2005 2:10:49 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/9 * DNIS:8729306 * CSID:9734676589 * DURATION (mm-ss):07-54

Aiello 1999-0053

As for the claims that depend on claim 34 (8-11 and 35-39), it is respectfully submitted that they are not anticipated by Weinstein et al at least by virtue of their dependence on claim 34. It is also respectfully submitted that at least in connection with some of them the Examiner's comments are NOT on point. For example, in connection with claim 9 the Examiner makes the unsupported statement that Weinstein et al "show any number of said keys taken from the set consisting of K, AK, and SK are symmetric keys...," but the Examiner has not shown the creation of such keys in the first place. In connection with claim 10 the Examiner points to a passage that basically teaches the fact that public keys exists, without tying it to any particular key of the method, and clearly without tying to the key K. In connection with claim 11 the Examiner points to a passage at col. 11, line 6, which teaches that MAC is generated by performing a hash. That, however, does not teach that a hash is "included with **each** transmission" (emphasis supplied). Lastly, in connection with claim 38 the Examiner points to col. 4, lines 65-67, but the cited passage teaches:

> The connection is private. Encryption is used after an initial handshake to define a secret key. Symmetric cryptography is used for data encryption (e.g. DES and RC4).

This does NOT teach that the information is encrypted with key SK, which was created by BTI, and in connection with which BTI sent the complement key SK^{-1} to the server.

Claims 2-7 were rejected under 35 USC 103 as being unpatentable over Weinstein et al in view of Quatrano et al, US Patent 6,675,216. Applicants respectfully traverse.

Basically, the Examiner cites the Quantrano et al reference for its teaching of voice communication. Such teaching, however, does not supply that which is missing in Weinstein et al, as discussed above. Therefore, combining Quantrano et al with Weinstein et al does not render claims 2-7 obvious.

Claim 12 was rejected under 35 USC 102 as being anticipated by Weinstein et al. The Examiner asserts that Weinstein et al teach a processor that executes program instructions as specified in the claim. Those program instructions parallel, to a substantial extent, the method defined in claim 34. Therefore, the arguments presented in connection with claim 34 apply to claim 12. Consequently, applicants respectfully submit that claim 12 is not anticipated by Weinstein et al. Since independent claim 12 is

PAGE 17/18 * RCVD AT 4/25/2005 2:10:49 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/9 * DNIS:8729306 * CSID:9734676589 * DURATION (mm-ss):07-54

not anticipated by Weinstein et al, it follows that claims 13-15, 18-20, and 22 are not anticipated by Weinstein et al.

In light of the above remarks, applicants respectfully submit that all of the Examiner's objections and rejections have been overcome. Reconsideration and allowance are respectfully solicited.

Respectfully,
William A. Aiello
Charles R. Kalmanek
Steven Michael Bellovin
William Todd Marshall
Aviel D. Rubin

Dated: 4/25/05

By _____
Henry T. Brendzel
Reg. No. 26,844
Phone (973) 467-2025
Fax (973) 467-6589
email brendzel@comcast.net

PAGE 18/18 * RCVD AT 4/25/2005 2:10:49 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/9 * DNIS:8729306 * CSID:9734676589 * DURATION (mm-ss):07-54